REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicant has amended claims 1, 10, and 18. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-3, 5-12 and 14-20 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 102(b)

Claims 1-3, 5-12 and 14-20 stand rejected under 35 U.S.C. 102(b) as being anticipated by Asokan et al. (Reference U: "Authenticating public terminals"). Applicant respectfully disagrees.

Asokan discloses public untrusted terminals which are used to access computer systems. Asokan discloses different ways for a user to authenticate a public terminal before using it to process sensitive information. (Asokan, Abstract)

The Examiner's attention is directed to the fact that Asokan fails to at least teach a "first institution", a "second institution", and that "the first device is a trusted device and the first characteristic relates to an access legitimization legitimating the first device for accessing a first institution", as recited in independent claims 1, 10, and 18.

The present invention discloses, in one embodiment, the second characteristic of the second device comprises an identifier identifying the second device. Access to a second institution is granted to or via the second device based on the associating of the first characteristic relating to the access legitimization and the second characteristic comprising the identifier. The second institution can be identical to or different from the first institution. Agreements can ensure that an access legitimization for accessing the first institution legitimates also for access to the second institution. Thus, the associating of the characteristic relating to the access legitimization and the second characteristic comprising the identifier for identifying the second device can provide the information that the second device is legitimated for accessing the second institution. Based on that information, access to the second institution can be granted. An access assertion may be sent from the server to the second device, to the second institution or a further entity

supporting the second device or the second institution for granting access. The access assertion may comprise an access legitimization that legitimates for accessing the second institution which can be e.g. derived from the access legitimization that legitimates for accessing the first institution. Access to the second institution can be e.g. achieved by unlocking the second device for appropriate usage. (Applicant's published Specification, [0024]

In contrast, Asokan fails to provide a teaching of a first institution and a second institution. Asokan does not teach using an access legitimization legitimizing access to a first institution for granting access to a second institution for or via a second device since, according to Asokan, access can only be granted via a terminal to a server. The present invention is based on a dual institution concept (i.e., "first institution" and "second institution" of the present claims). This concept is not disclosed or contemplated by Asokan. The dual institution concept requires inter alia that an access legitimization legitimating the trusted device to access a first institution is related to a first characteristic of the trusted device, that the access legitimization is verified for executing the linking as a prerequisite for the execution of the linking (to which also the successful completion of the association of the characteristics belongs), and that a message is sent for granting access to the second institution. Hence, according to the present invention as claimed, an access legitimization legitimating for access to a first institution is used to gain access to a second institution. Clearly, this dual institution concept is not contemplated by Asokan.

Applicant's claims presently recite that "the first device is a trusted device and the first characteristic relates to an access legitimization legitimating the first device for accessing a first institution". It appears that the Examiner is reading the user, his trusted personal device and the terminal of Asokan as the first institution and the central server of Asokan as the second institution. Asokan clearly does not teach a first (trusted) device for accessing a first institution, as recited by Applicant's claims. On the contrary, the Examiner argues that the trusted personal device of Asokan **is** the first institution. As such, it is clear that Asokan fails to teach what is recited by Applicant's claims.

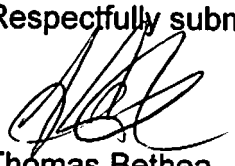
In view of the above arguments, Applicant respectfully asserts that independent claims 1, 10, and 18 are patentable over Asokan. Dependent claims 2, 3, 5-9, 11, 12, 14-17, 19, and 20 are patentable at least by virtue of depending from their respective base claim.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Thomas Bethea, Jr
Registration No. 53,987

Date: October 5, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-4859
thomas.bethea.jr@ericsson.com